Amendments to the Drawings

Please replace the drawing sheet currently on file containing Figure 1, with the replacement sheet containing an amended Figure 1, submitted herewith.

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Amendments to the Specification

The specification is amended to correct several typographical errors. The specification is also amended replacing the character "l", which represents a bitstring of a predetermined length (introduced at paragraph [0033]), with its uppercase alternative "L" in order to distinguish same from the numeral 1 (one). The character "l" was chosen to represent an arbitrary value for the length of the bitstring. Applicant believes that the uppercase alternative is an appropriate substitute, and in no way adds subject matter to the subject application. Applicant advises that each instance of "l" has been amended accordingly for consistency.

Amendments to the Claims

Various typographical errors are amended in the claims, and the character "l" has been replaced by "L" in each instance, consistent with the above amendments to the specification. No new matter is added by way of these amendments.

Amendments to the Drawings

Figure 1 is amended to include the reference numerals "10" and "16" as recited in paragraph [0028] of the specification. No new matter is added by way of these amendments.

Oath/Declaration

The Examiner believes that the oath or declaration for the present application is defective, particularly that it does not identify this application by application number and filing date (MPEP §602.01 and §602.02), and is not signed by the inventors. Applicant advises that a combined Declaration and Power of Attorney meeting the above requirements was filed on February 12, 2002. However, Applicant respectfully re-submits a copy of said document with this response.

Objections to the Drawings

The Examiner rejected the Figures for failing to comply with 37 CFR 1.84(p)(5), specifically for failing to identify reference numerals "10" and "16" mentioned in the

specification. Accordingly, Figure 1 is amended to include numerals 10 and 16 consistent with paragraph [0028] of the specification. Applicant believes the drawings comply with 37 1.84(p)(5), and are of acceptable form.

Claim Rejections – 35 U.S.C §102(b)

Claims 1-2 and 4-5 have been rejected under 35 U.S.C. §102(b) as being anticipated by Schneier "Applied Cryptography", pages 483-490 (hereinafter "Schneier"). Applicant respectfully traverses the rejections as follows.

In paragraphs [0013] to [0017] of the subject application, the implementation of the Digital Signature Algorithm (DSA) is discussed, specifically, a bias that is introduced in the selection of the key k. This bias may be exploited to extract a value of, e.g., the private key d and thereafter render the security of the system vulnerable (see paragraph [0013]). Moreover, the work of Daniel Bleichenbacher is discussed in paragraph [0017], which suggests that the modular reduction to obtain k introduces sufficient bias into the selection of k, such that an examination of 2^{22} signatures could yield the private key d in 2^{64} steps, using 2^{40} memory units. Bleichenbacher's work suggests that the key k need be chosen carefully, or the above vulnerability may be exploited.

The present invention provides a key generation technique that intends to eliminate such a bias during the selection of the key. In particular, claim 1 recites a method of generating a key over a group of order q, having the following steps:

(a) generating a seed value from a random number generator;

(b) performing a hash function on said seed value to provide an output;

(c) determining whether said output is less than said prime number q;

(d) accepting said output for use as a key if the value thereof is less than said prime number q; and

(e) rejecting said output as a key if said value is not less than said order q.

[identifiers added for discussion purposes herein only]

Applicant respectfully submits that Schneier does not teach all steps of claim 1 recited above, and therefore, cannot anticipate claim 1.

Schneier describes the DSA that was proposed for use in the Digital Signature Standard (DSS) by the National Institute of Standards and Technology (NIST). The Examiner relies on

the following passages: page 487, lines 7-15; and page 489, lines 15-18. On page 487, Schneier discusses a procedure for signing and then verifying a message. There is defined, among others, a private key x, a public key y, a message m, a random number k, and a value q. To sign the message m, Alice first generates a random number k that is less than q. The Examiner believes that this step is equivalent to step (c) above. Applicant respectfully disagrees, and believes that the Examiner has misconstrued what Schneier teaches in this passage.

Step (c) of claim 1 involves determining whether the output is less than q, where the output is a result of a hash on a seed number that is chosen at random. In Schneier, k is a random number that is generated by Alice, and is said to be less than q. This value k is not an output that is a result of a hash on a seed number chosen at random, it is a random number in itself. In fact, k is actually an input used in generating a signature, not an output that is compared with a prime number q for generating a key. Moreover, no comparison is even performed in this step by Schneier. In claim 1, the comparison of the output with q is done so to exclude keys that have the vulnerability discussed above. Schneier simply does not teach such a step.

Moreover, the Examiner believes that lines 12-15 of the passage of page 487 teaches step (d) above. Applicant believes this is entirely incorrect. At lines 12-15, Schneier describes generating signature components r and s. Schneier does not teach accepting an output as a key if its value is less than q. A key has not even been generated by Schneier in these steps. Signature components are in fact created for signing the message m.

The passage taken from page 489 includes steps of checking whether or not q is prime. This in no way teaches the step of determining whether an output is less than a prime q. In fact, Schneier teaches the determination of the nature of q, not a comparison with another value.

Applicant believes that the Examiner has misconstrued the teachings of Schneier. Schneier does not teach at least steps (c) and (d) recited above. Accordingly, Schneier cannot anticipate claim 1. Therefore, claim 1 is believed to be patentable over Schneier. Claims 2 and 4-5 are dependent on claim 1, and as such are also believed to be patentable over Schneier.

Claim Rejections – 35 U.S.C. §103(a)

Claims 7-13

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over

Schneier, in view of US Patent No. 6,219,421 to Backal. Applicant respectfully traverses the rejections as follows.

Firstly, claim 7 is dependent on claim 1, and claim 8 is dependent on claim 7. Applicant has shown above that Schneier does not anticipate claim 1. The Examiner has indicated that Schneier does not teach the subject matter of claims 7 and 8. In order to establish a *prima facie* case of obviousness, one of the criteria that must be met is that the references relied upon must teach all elements of the claim (§2143 MPEP). For the combination relied upon by the Examiner to teach all elements of claims 7 and 8, Backal would not only have to teach the subject matter of claims 7 and 8, but also what is missing from Schneier regarding claim 1. Applicant respectfully submits that Backal does not teach what is missing from claim 1, and for at least that reason, claims 7 and 8 are patentable over the combination of Schneier and Backal.

Backal teaches a virtual key method using a virtual matrix to avoid sending large keys over a communication channel. Backal does not teach the step of determining whether an output is less than a prime number q, where the output is provided by performing a hash function on a seed value generated at random. Backal also does not teach the step of accepting the output as a key if the value thereof is less than q. Accordingly, Backal does not teach what is missing from Schneier. Therefore, Applicant believes that claims 7 and 8 are patentable over the combination of Schneier and Backal.

Secondly, claim 9 is an independent claim that, in part, teaches the step of determining whether an output has a value less than q. As shown above, neither Schneier nor Backal teach such a step. Therefore, for at least that reason, Applicant believes that claim 9 is patentable over the combination of Schneier and Backal. Claims 10-13 are either directly or indirectly dependent on claim 9, and as such, are also believed to be patentable over the combination of Schneier and Backal.

In summary, Applicant respectfully submits that neither Schneier, nor Backal teaches a step of determining whether an output is less than a prime number q, and therefore, for at least that reason, claims 7-13 are patentable over such a combination.

Claims 3 & 6

Claims 3 and 6 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, in view of Nel et al. "Generation of Keys for use with the Digital Signature Standard

(DSS)", pages 6-10 (hereinafter "Nel"). Applicant respectfully traverses the rejections as follows.

Claims 3 and 6 are both dependent on claim 1. Applicant has shown above that Schneier does not anticipate claim 1. The Examiner has indicated that Schneier does not teach the subject matter of claims 3 and 6. Therefore, similar to the above, Nel must not only teach the subject matter of claims 3 and 6, but also what is missing from Schneier regarding claim 1. Applicant respectfully submits that Nel does not teach what is missing from claim 1, and for at least that reason, claims 3 and 6 are patentable over the combination of Schneier and Nel.

Nel teaches key generation for the DSS, specifically, a summary of the private-key generation method found in the original draft DSA proposal by NIST. In section 5.B, *viz.*, the critically flawed step of $k = G(t, XKEY) \bmod q$ is shown. This reduction modulo q introduces the bias discussed earlier in the value k. The present invention avoids this bias by rejecting values for a key that are not less than q, in part, using the step of determining whether an output is less than the prime number q. Nel does not teach such a step, but in fact teaches the vulnerability that the present invention avoids. Nel in no way teaches the step of determining whether an output (to potentially be used as a key) is less than the prime number q.

Accordingly, Nel does not teach what is missing from Schneier. Therefore, for at least that reason, Applicant believes that claims 3 and 6 are patentable over the combination of Schneier and Nel.

Claim 14

Claim 14 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, in view of Backal, and further in view of Nel. Applicant respectfully traverses the rejection as follows.

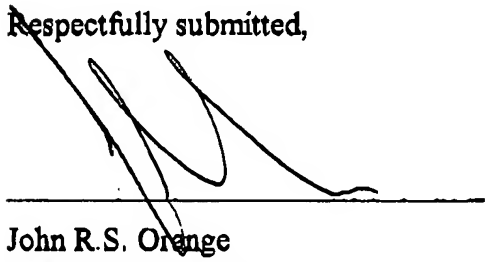
Claim 14 is dependent on claim 9. Applicant has shown above that none of Schneier, Backal, nor Nel teach a step of determining whether an output is less than a prime number q. Accordingly, the combination of Schneier, Backal and Nel does not teach all of the subject matter of claim 1, let alone claim 9, which is dependent on claim 1. Therefore, for at least that reason, Applicant believes that claim 14 is patentable over the combination of prior art cited by the Examiner.

Summary

In view of the foregoing, Applicant believes that claims 1-14 clearly and patentably distinguish over the prior art relied upon by the Examiner, and are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: September 22 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL